What is claimed is:

1. A process that monitors network traffic through a monitoring device disposed between a data center and a network for thwarting denial of service attacks on the data center comprises:

a detection process to determine if the values of a parameter exceed normal values for the parameter to indicate an attack on the site;

a characterization process to build a histogram for the parameter to compute significant outliers in a parameter and classify the attack; and

a filtering process that provides filtering of network packets based on characteristics of the attack.

2. The process of claim 1 wherein suspicious parameter values are represented by a bit vector with a 1 in every position corresponding to a "bad" value, and a 0 in every position corresponding to a "good" value.

3. The process of claim 1 wherein the characterization process comprises:

a correlation process that correlates suspicious parameters and determines existence of correlations of those parameters that can point to types of attacks.

4. The process of claim 3 wherein the correlation process is used to reduce dropping of legitimate traffic.

5. The process of claim 2 wherein filtering is aggregate filtering.

6. The process of claim 1 wherein parameters include at least one of source IP address, destination IP address, source TCP/UDP ports, destination TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload fragment, IP TOS field, and TCP flags.

7. A method for thwarting denial of service attacks on a data center, the method comprising:

producing a histogram of received network traffic for at least one parameter of network packets; and

characterizing an attack based on comparison of historical histograms with the produced histogram data for one or more parameters.

8. The method of claim 7 further comprising:

filtering network packets sent to the data center based on whether or not a value of the attribute represented in the histogram is within a normal range of values for the attribute.

9. The method of claim 7 wherein historical histograms are based on time periods that can range from 1 hour to 1 week or more.

10. The method of claim 7 wherein produced histograms are produced during an attack and over time periods of about 10-300 sec or so.

11. The method of claim 7 further comprising:

normalizing the two histograms for each parameter; and

computing their difference to identify significant

outliers that are considered indicators of suspicious traffic.

12. The method of claim 11 further comprising:

correlating suspicious parameters to reduce blocking of legitimate traffic.

13. The method of claim 12 wherein the bit vector contains sufficient bits to represent the whole parameter space.

14. The method of claim 11 further comprising:

correlating suspicious parameters to determine existence of correlations of those parameters that can point to indications of attacks.

15. The method of claim 11 wherein filtering based on attribute further comprises:

producing a master correlation vector from a stream of sampled packets and examining the network packets using a process that is constant-time, independently of the number of correlations or of the number of suspicious values for a parameter.

16. The method of claim 11 wherein filtering based on attribute further comprises:

constructing a master correlation bit vector corresponding to the most important parameter correlations; and

producing for each packet a correlation bit vector to index into the master correlation bit vector.

17. The method of claim 16 wherein filtering based on attribute further comprises:

testing the bit in the master correlation vector to decide whether to drop or forward the packet.

18. The method of claim 7 wherein attributes include at least one of source IP address, destination IP address, source TCP/UDP ports, destination TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload fragment, IP TOS field, and TCP flags.

19. The method of claim 7 wherein the method is executed on a data collector.

20. The method of claim 7 wherein the method is executed on a gateway.

21. A monitoring device for thwarting denial of service attacks on a data center, the monitoring device comprises:

a computing device executing:

a process to build at least one histogram for at least one parameter of network traffic; and

a process to characterize an attack based on a comparison of a historical histogram of the at least one parameter to the built at least one histogram for the at least one parameter.

22. The monitoring device of claim 21 further comprising:

a process to correlate suspicious parameters to reduce blocking of legitimate traffic.

23. The monitoring device of claim 21 wherein the characterization process normalizes the historical and built histograms for each parameter and computes their difference to identify significant outliers that are considered indicators of suspicious traffic.

24. The monitoring device of claim 23 wherein the characterization process produces a master correlation vector from a stream of sampled packets and examines the sampled packets using a process that is constant-time, independently of the number of correlations or of the number of suspicious values for a parameter.

25. The monitoring device of claim 21 wherein the device is a gateway device that is adaptable to dynamically install filters on nearby routers.

26. The monitoring device of claim 21 wherein the device is a data collector.

27. The monitoring device of claim 21 wherein the parameters include at least one of source IP address, destination IP address, source TCP/UDP ports, destination TCP/UDP ports, IP protocol, IP TTL, IP length, hash of payload fragment, IP TOS field, and TCP flags.

28. A computer program product residing on a computer readable medium comprising instructions for causing a processor to:

build a histogram for any attribute or function of a parameter of network traffic; and

use the histogram data for the parameter to characterize an attack on the site.

29. The computer program product of claim 28 further comprising instructions to:

filter network traffic based on characterization of the attack.

30. The computer program product of claim 28 further comprising instructions to:

determine if the values of a parameter exceed normal values for the parameter to indicate an attack on the site;

31. The computer program product of claim 30 further comprising instructions to:

use the histogram to characterize the attack when it is determined that one of the parameters exceeds a threshold.

32. A method of protecting a victim site during a denial of service attack, comprises:

disposing a gateway device between the victim site and a network;

monitoring network traffic through the gateway and determining if values of at least one parameter exceed normal, threshold values expected for the parameter to indicate an attack on the site;

producing a histogram for the at least one parameter of network traffic to characterize the attack by comparing the histogram to at least one historical histogram for that parameter; and

filtering out traffic based on characterizing the traffic, which the gateway deems to be part of an attack.

33. The method of claim 32 further comprising:

communicating statistics collected in the gateway to a control center.

34. The method of claim 33 wherein communicating occurs over a dedicated link to the control center via a hardened network.

35. The method of claim 33 wherein the gateway is physically deployed in line in the network.

36. The method of claim 33 wherein filtering occurs on nearby routers.

37. A method to reduce blocking of legitimate traffic in a process to protect a victim site during a denial of service attack, comprises:

producing a histogram of network traffic to characterize an attack; and

filtering out traffic deemed part of an attack with filtering comprising:

constructing a master correlation vector having asserted bits corresponding to the most important parameter correlations;

initializing a packet's correlation bit vector to 0, and for every parameter:

retrieving the parameter in a parameter suspicious vector to construct the packet' correlation bit vector; and

using the value of the packet's correlation bit vector to index into the master correlation bit vector.

38. The method of claim 37 further comprising:

testing the indexed bit in the master correlation vector, where if the bit in the master correlation bit vector is a one, the packet is dropped, otherwise the packet is forwarded.

39. The method of claim 37 wherein the master correlation vector is constructed from a stream of sampled packets.

40. The method of claim 37 further comprising:

maintaining a correlation bit vector with as many bits as there are parameters; and

if a parameter's suspicious vector has a 1 in a bit position corresponding to the parameter's value in a packet, the method further comprises:

setting the bit corresponding to the parameter in the packet's correlation vector to 1.